Link Management Security in Bluetooth

Sampat Das

Roll. 710cs2178

under the direction of

Dr. Ashok Kumar Turuk

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Link Management Security in Bluetooth

Submitted in

June 2015

to the department of

Computer Science and Engineering

of

National Institute of Technology Rourkela

in partial fulfillment of the requirements

for the degree of

Master of Technology

by

Sampat Das

(Roll. 710cs2178)

under the direction of

Dr. Ashok Kumar Turuk

Department of Computer Science and Engineering

National Institute of Technology Rourkela

Rourkela – 769 008, India

Department of Computer Science and Engineering

National Institute of Technology, Rourkela 769008

CERTIFICATE

This is to certify that the thesis entitled **Link Management Security in Bluetooth** submitted by **Sampat Das** in partial fulfillment of the requirements for the grant of the degree of **Master of Technology** in **Computer Science and Engineering** with specialization in **Information Security** to the **National Institute of Technology, Rourkela** is a genuine record of research work done by him under my supervision. The contents of this thesis have not been submitted to any other university or institute for the grant of any degree or diploma.

Thesis Advisor

Dr. A.K.Turuk

Associate Professor

Department of Computer Science and Engineering

DECLARATION

I hereby pronounce that all the work contained in this thesis is my own specific work unless otherwise recognized. Also, all of my work has not been previously submitted for any scholarly degree. All sources of quoted information have been recognized by proper method of references.

Sampat Das
710cs2178
NIT Rourkela

ACKNOWLEDGEMENT

First of all I want to express my sincere gratitude to my guide **Prof. A.K.Turuk** Sir for his consistent support and motivation.Without his backing and inspiration I would not have completed by project work. His steady inspiration kept me passionate for my research work.His ideas and knowledge really helped me a lot in going to a deeper level of understanding and achieving my goal.

I would also like to express my gratitude to our HOD **Prof.S.K.Rath** Sir for his invaluable tips and advices. I also want to thank all my friends and my batchmates and all those who are directly or indirectly related to my work anyway.

Last, but not the least, I would like to thank my Mom and Dad and would like to dedicate my everything to them because without them nothing would have been possible as they have supported me in every situation I have faced in life.

Sampat Das

710cs2178

ABSTRACT

Bluetooth is a very useful and low cost wireless technology which has been developed for transferring data over short distances.Bluetooth is nowadays widely used for many purposes like file transfer, communicating with mouse and keyboard, listening to audio and many other applications. Bluetooth has many advantages over the other wireless networks such as Wi-Fi and Infrared. Security is a major concern in bluetooth as all the security options have not been explored in this wireless technology. Diffie Hellman protocol is a widely used protocol in the field of network security. But this protocol is basically a key exchange protocol and is applied during the exchange of keys

In this thesis the diffie hellman protocol is applied on the random number, which is directly sent from the verifier to claimant, rather than the key itself.Then this random number is used for generating the keys.Sending the random number directly can cause security issues as the random number, bluetooth address and PIN can be known by the eavesdropper who can be a threat to the network. So this step improves the security of the bluetooth network.

***Keywords*:** Bluetooth Security, Diffie Hellman Protocol, Wireless Technology, Claimant, Verifier

Contents

List of Figures

Chapter 1

Introduction

1.1 Objective

Bluetooth is a low cost wireless technology which has been developed for transferring data over short distances.It was invented by Ericsson in 1994 and it is managed by a body named **Bluetooth Special Interest Group**. [18] [19] It is standardised as IEEE 802.15.1. Bluetooth works in 2400-2483 MHz. [18] This lies in the globally unlicensed Industrial, Scientific and Medical(ISM) 2.4 GHz Short range radio frequency band. Bluetooth basically uses a technology called Frequency-hopping spread spectrum. [18] In this technology the data are broken into small packets and then each packet is transmitted through one of the 79 channels of bluetooth. Each channel has been alloted a bandwidth of 1 MHz. [2] [9]

Bluetooth has a wide range of applications such as

- Tranferring files, contacts and other data
- Communication with the computer I/O Devices such as mouse, printer and keyboard
- Listening to audio files using a bluetooth headset
- Listening to voice over call using a bluetooth headset
- Communication between computers where little bandwidth is required

So basically bluetooth can be usefull to us in a lot of ways. But like any other wireless network Bluetooth Technology also has numerous security issues and loopholes. [21]The data that we transmit using the bluetooth wireless technology can be private or public.So if an intruder gets access to the private date it can bring about harm to the user.So to ensure a secured transmission we need to follow the best security protocols and we also need to work on the existing algorithms and protocols so as to improve upon them. [11] [19]

Figure 1.1: Bluetooth Connectivity

1.2 Project Overview

This project has been done on the Link Manager Protocol layer of the bluetooth which basically manages the logical link that is established between the devices before the transmission of any data and also deals with the authentication and encryption part of network.There is a standard algorithm by which the link and the encryption key are exchanged between the devices. This algorithm uses a random number which is sent by a device to the other device unencrypted via air. This random number is the main vulnerablity of the Bluetooth system. If an eavesdropper gets to know this random number he can be a threat to the system. So in our system instead of sending the random number directly we are using the diffie hellman protocol to do the same. So this improves the security of the system. For implementation JSR-82 simulator has been used. [4] It is the java specification request which is the official API for bluetooth in java. [6] [20]

1.3 Organization of the Thesis

The Thesis is organised as follows:

1. Chapter 1: In the chapter one we have introduced about the bluetooth and the inspiration behind working on this technology.
2. Chapter 2: In this chapter we go through the basics of bluetooth, how it is designed, how its security features are designed and all other facts related to bluetooth.
3. Chapter 3: In this chapter we have done literature review on bluetooth.
4. Chapter 4: In this chapter we have given the proposed method and the implementation details.
5. Chapter 5: This chapter is the conclusion chapter.

Chapter 2

Basics of Bluetooth Security

2.1 About Bluetooth

Bluetooth is a wireless technology which is gradually becoming popular nowadays because of its low cost and low power. It is replacing many other wireless technologies for short range wireless connectivity.Bluetooth hardware basically consists of a bluetooth radio chip embedded inside the system. This chip is responsible for transmitting the signal to the other device. For using the bluetooth technology a device must be consistent with the subset of the bluetooth profiles which are required to use any bluetooth service. So for both the devices to be working they need to support the required profile. A profile basically gives the standard for using a particular service. So to use all the services it is necessary for the device to support the respective profiles.
Some of the important profiles are [18]:-

- Generic Access Profile:-
  It is the first basic Bluetooth profile. It deals with the bluetooth discovery and connectivity and without this no other profile will work.

- Service Discovery Application Profile:-
  This profile tells how to discover different services on a remote device using the service discovery protocol. It helps in finding out what all services are there on the device it will connect to.

- Basic Imaging Profile:-
  This profile deals with the transferring of images between the two devices and it also has the capacity to resize and convert images to a different format so as to make them compatible with the receiving device.

- Basic Printing Profile:-
  This profile allows the device to send the files ,text, images and other items to the printing device to get a print out. So for printing any item using bluetooth we require this profile.

- File Transfer Profile :-
  This is the most important profile and is used for transferring of files and other items between two devices.

- Cordless Telephony Profile:-
  This allows the cordless phones to function using the bluetooth.

- Generic Object Exchange Profile:-
  This profile helps in transfer of an object from one device to other.

The Bluetooth Special Interest Group has defined many such profiles and each of these profiles is for a particular service and we need to use the profile for that service.

2.2 Bluetooth Protocol Stack

The Bluetooth architecture consists of a stack of protocols which is a combination of software and hardware implementation of all the protocols defined in the standard. It consists of many layers. Some layers are for software and some for hardware.All the layers are continuous and they work one after the other. The data passes through all the layers to reach to the end. So the different layers starting from the bottom are :- [18]

- Radio Frequency Layer :-
  The radio signals are processed in this layer. This layer is resposible for physical transmission of signals. This layer uses a technology named frequency hopping spread spectrum . In this the data are broken into small packets and each small packet is sent through one of the 79 channels allocated for bluetooth .Bandwidth of each channel is 1MHz. [18]

- Baseband Layer :-
  This layer helps in the physical connection between the two devices.

Formatting of the packets is done in this layer like header,checksum calculation etc.

- Link Manager Layer :-
  This layer is responsible for the logical link establishment between different devices. The devices can exchange files with each other only after establishing a link or connection and this layer helps in this. All the security features are also implemented in this layer such as encryption and authentication. The Link Keys are also established int this layer.

- Logical Link Control and Adaptation Protocol :-
  It is a very important layer and it implements many powerful features. Segmentation of packets and Data reassembling are done in this layer. A very large data is broken into smaller ones in this layer.

- Host Controller Interface :-
  This layer is an interface between the hardware and software part of the bluetooth. This layer passes all the data from the computer to the embedded bluetooth chip.

- Service discovery Protocol :-
  This protocol is used by a device to search for different services in the other remote device. For example if we want to print any file, the printer will be searched using this protocol.

- Object exchange Protocol :-
  This protocol helps in the exchange of objects between the devices. Normal file exchanges also use this protocol.

- Radio Frequency Communication: -
  This protocol is basically used for cable replacement .It emulates the EIA-232 and is used to create a virtual data stream.

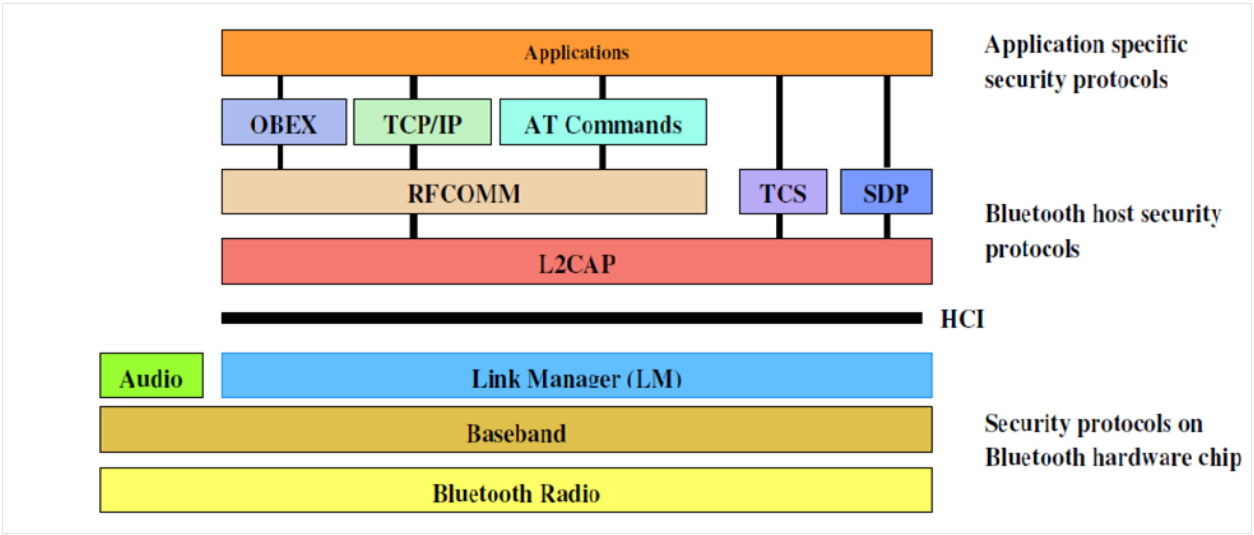

Figure 2.1: Bluetooth Protocol Stack

These were some of the core protocols and the figure depicting them is given above.

2.3 Attacks on Bluetooth

- MAC Spoofing Attack :-

  Attackers can perform spoofing before the authentication process takes place.They can spoof a particular MAC address and can impersonate some one. This attack is very dangerous and is a threat to security. [12]

- PIN Cracking Attack :-

  The random number is sent unencrypted from one device to the other. An attacker can easily take that random number, the bluetooth address and can crack the possbile value of pin using permutation and can easily get the initialization key which is used during authentication. [12]

- Man in Middle Attack :-

In this type of attack an eavesdropper can manipulate the messages which are sent between the two devices making them believe that they are connected to each other but they are not. Also known as impersonation attack. [12] [3] [13]

- Denial of Service Attack :-
  In this the attacker can crash a device by flooding it with innumerable requests. Finally the security is compromised. This attack is common in other wireless networks also. [12] [13]

  These are the primary attacks on a bluetooth device. In our thesis we have dealt with the PIN cracking attack and we have proposed a method to make a bluetooth device more safe from this attack.

2.4 Link Manager Protocol

The Link Manager Layer is the layer where we are working in. This link manager is resposible for controlling the logical link.It deals with all the activities related to setup and cofiguration of the link. The security protocols are also implemented by the link manager layer.The Link Manager is also responsible for sharing a type of message know as control message which is also known as **Protocol Data Unit**. [15] These control messages usually are security related and they also carry information necessary for authentication and encryption.

Link is bacsically the channel that has been created between the two devices. The devices can exchange items between each other only when a proper link has been established. To ensure a proper link between two devices the authentication procedure takes place. Only after a proper authentication procedure the link gets created and then the encryption takes place and the item gets exchanged.For the authentication procedure the initialization key and the link key are used.

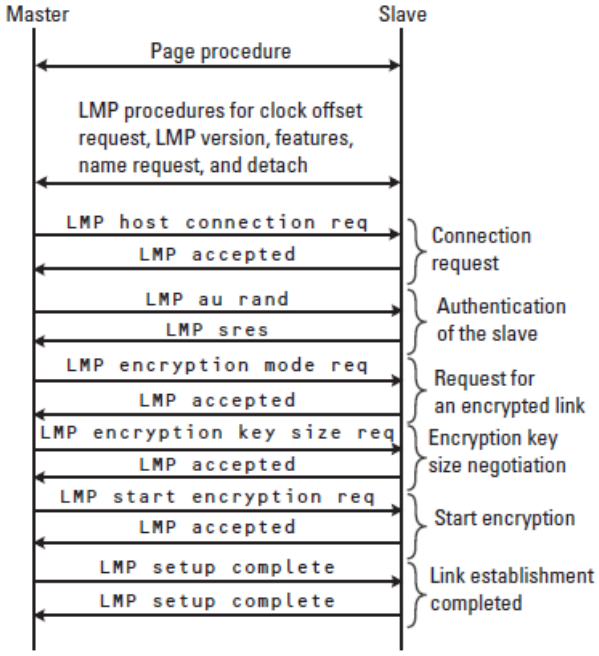

Figure 2.2: LMP Protocol Data Unit flow

2.5 Authentication

The first operation that is done is pairing. The link key is generated during this step. Once the link key gets exchanged between the two devices the pairing is done and hence the authentication.

The pairing procedure consists of the following steps:- [5] [15] [16] [12]

- Initialization Key Generation
- Link Key Generation
- Exchange of Link Key
- Authentication

2.5.1 Initialization Key Generation

The initialization key is always formed when any two devices meet for the very first time. Every device comes with a pre set bluetooth address manufactured from the factory. It is represented by BD_ADDR which is a 48 bit number. For generation of an initialization key a random number IN_RAND is sent by the device A to the device B where the device B has approached the device A for file exchange. So in order to authenticate the device B the device A sends a random number of 128 bits. Then the device B forms an initialization key using the random number IN_RAND, the bluetooth address of BD_ADDR and the PIN number that is given by the user.

$$K_{INIT} = E_{22}(PKEY^{'}, IN\_RAND, L^{'}_{PKEY})$$

where [15] [12] [7] [1]

$$L^{'}_{PKEY} = min(L_{PKEY} + 6, 16)$$

$$PKEY^{'}{=}PKEY \cup BD\_ADDR \text{ if } L_{PKEY} \leq 10$$
$$PKEY^{'}{=}PKEY \cup BD\_ADDR[0...(15 - L)] \text{ if } 10 \leq L_{PKEY} \leq 15$$
$$PKEY^{'}{=}PKEY \text{ if } L_{PKEY} = 16$$

E_{22} [15] [12] [7] is a pre defined bluetooth algorithm and it is a variation of the SAFER+ algorithm.
$PKEY^{'}$ [15] [12] [7] is the pass key
L_{PKEY} [15] [12] [7] is the length of the pass key.

2.5.2 Generation and exchange of link key

The initialization key K_{INIT} is used in the generation of the link key. In our work we have considered the unit key to be the link key. Now device A sends the random number to device B and it forms the initialization key. The device B also forms the unit key i.e K_B . The unit key is formed from the bluetooth address of B

and another 128 bit random number LK_RAND_B with the help of a predefined bluetooth algorithm E_{21}. [15] [12]

$$K_B = E_{21}(LK\_RAND_B, BD\_ADDR_B)$$

Once this unit key is formed it is then sent to the device A by XORing $\bigoplus$ it with the initialization key K_{INIT} .

$$K_B^{'} = K_B \bigoplus K_{INIT}$$

Now the device A can calculate the initialization key as it is a function of the random number generated by A, Bluetooth Address of B and the pass key. So the device A has the initialization key. So he can simply get the link key or the unit key K_B by using the property of the XOR fucntion.

$$K_B^{'} \bigoplus K_{INIT} = K_B \bigoplus K_{INIT} \bigoplus K_{INIT} = K_B$$

So in this manner the the device A also gets to know the value of K_B . So finally the unit key or the link key gets exchanged between the two bluetooth devices. So this key is secret between the two devices and is known only to them. So only when it is confirmed that both the devices share the same link key then only the pairing is done. So this takes place in the authentication process.

2.5.3 Authentication

The authentication process consists of a verifier and a claimant. Device A is the verifier and Device B is the claimant. Now for authentication purpose the device A challenges the device B and expects a response from it. A sends 128 bit random number AU_RAND to B. The device B using its bluetooth address BD_ADDR_B , the random number and the link key K_B that was shared between them calculates a response $SRES$ and then sends it back to A. If it matches with that of A both the devices get authenticated to each other. [15] [8] [10]

$$SRES = E_1(K_B, AU\_RAND, BD\_ADDR_B)$$

This response should be the same as calculated by device A.

So this is the last step of pairing. After the authentication process the pairing is done. Now the link key which is used in the pairing process is also used as a parameter in the generation of encryption key discussed in the next section.

2.6 Encryption and File transfer

The encryption key K_C is generated with the help of the link key K_B shared during authentication process, a 96 bit ciphering offset COF [15] [5] which is calculated during the authentication process and a 128 bit random number EN_RAND. It is calculated with an algorithm E_3 which is a pre defined and standard algorithm used in bluetooth systems. [10]

$$K_c = (K_B, EN\_RAND, COF)$$

This encryption key is then used to encrypt the packets which is done with the help of a stream cipher.Finally the data gets exchanged.

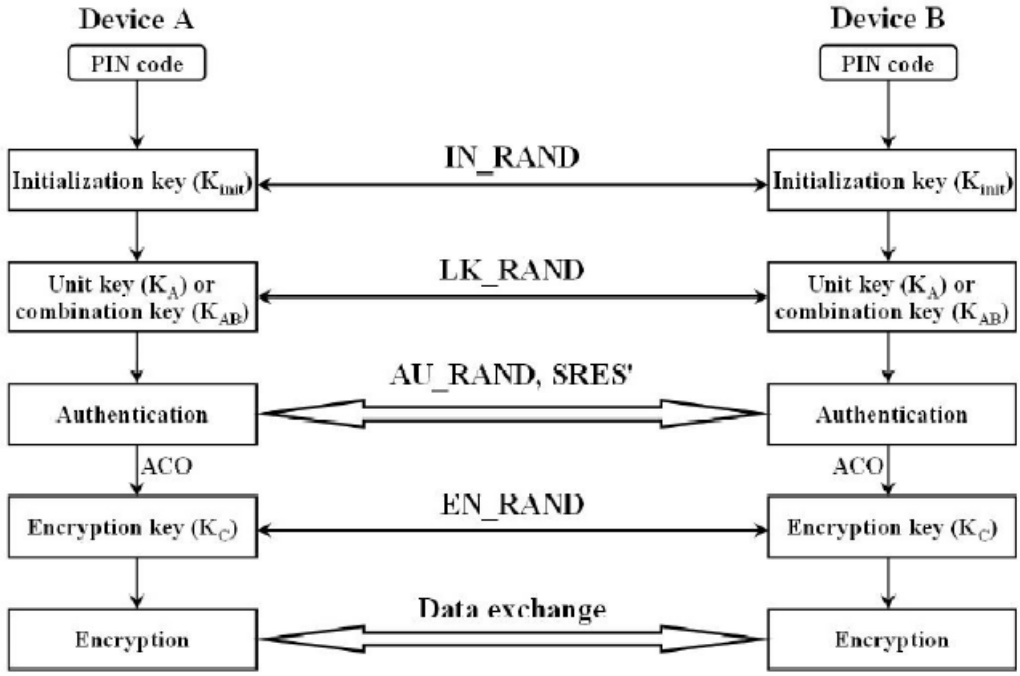

Figure 2.3: Bluetooth Data Exchange

Chapter 3

Literature Review

Bluetooth is a newer technology as compared to LAN and Wi-Fi. I have read some of the research papers and done the review.In this chapter I have given a brief summary of few of the papers that I have gone through.

3.1 Review of Research Papers

An analysis of Bluetooth Security Vulnerabilities-2003 [5]

The research paper basically describes about the security vulnerabilities of the bluetooth systems. It describes a methodology known as VERDICT which is used to determine the vulnerabilities of the bluetooth system and compare them with those of wireless LAN. This VERDICT [5] is used to identify weaknesses in authentication, encryption and key generation. Verdict is an abbreviation for Validation, Exposure, Randomness, Deallocation, Improper Conditions Taxonomy. [5]

- Validation:-

  Validation is the most important part of any security system. Any external input or device that we consider should be properly validated. Improper validation can cause havoc to the system. For example, Bluetooth Address of a device should be properly validated. Each bluetooth device has its unique address. If the address is not validated it may cause damage to the security of the system.

- Exposure:-

  This basically means how much the device is exposed. Improper exposure can allow a device to enter the network and effect the security of the system.The things which are not to be made public should not be made public.

- Randomness:-

  The role of random number is very much critical to the generation of different keys such as unit keys and combination keys. Therefore proper randomness should be ensured while generation of random numbers. When the random

numbers are not generated by proper algorithms an intruder can guess it and then crack the system.

- Deallocation:-

  Proper deallocation means removal of all the data residuals previously stored. Improper deallocation can cause havoc to the security of the system.For example, If the pointer is not deallocated after its use ,the dangling pointer may cause damage to the system. So proper deallocation of resources after their use is very much necessary.

The authors have done the VERDICT analysis and they have come to the conclusion that bluetooth system has weaknesses related to the improper validation,unnecessary exposure and randomness. Our proposal basically concentrates on the improper randomness. The random number generation before the link key is a potential threat to the system and we have dealt with this thing in our work.

Enhancing Bluetooth Authentication using Diffie Hellman Algorithm -2013 [17]

This paper demonstrates the use of Diffie- Hellman protocol. All the bluetooth systems follow a standard protocol for transfer of any item. First they generate an initialization key then the link key and then the encryption key.The initialization key is generated with the help of a random number, bluetooth address and the pass key. This paper says instead of doing this we can generate the initialization key using the diffie hellman protocol and then we can follow the rest of the procedure as it is.The diffie hellman protocol is safe from many threats and attacks. But the main problem here is that this protocol is also vulnerable to man in the middle attack. So an intruder can easily crack the initialization key. So we have worked on this drawback and we have applied the Diffie Hellman protocol on the random number rather than the key itself. So applying it on the random number i.e one step behind will make it more secure. Then this random number can be used to

generate the keys.

Bluetooth Security Threats and Solutions: A Survey 2012 [12]

This paper gives the complete survey of the bluetooth security.It discusses about the protocol stack. Detail regarding every layer has been presented starting fro the physicalm layer till the application layer. This paper has also discussed about the security architecture of the bluetooth. Bluetooth discovery and connectivity is divided into three modes of opertion :-

- Silent : In this mode the device will never accept any connection and it will simply keep the track of bluetooth traffic.
- Private : In this mode also the bluetooth device cannot be discovered .It will accept the request for connection only if the other device has its 48 bit bluetooth address.
- Public : In this mode the device can be easily discovered and can be connected to.Hence this mode is known as discoverable mode.

This paper also demonstrates the complete procedure of bluetooth transfer starting from the initialization key and link key generation to encryption. It also explores some of the existing network vulnerabilities and different types of attacks possible on bluetooth network. It also compares the vulnerabilities of all the versions of bluetooth released till now.So this paper is basically a complete overview of the whole bluetooth system.

3.2 Summary

This was the brief summary about some of the papers that were read by me. These papers helped me a lot to understand the bluetooth system and come to some conclusion.

Chapter 4

The Proposal and Implementation

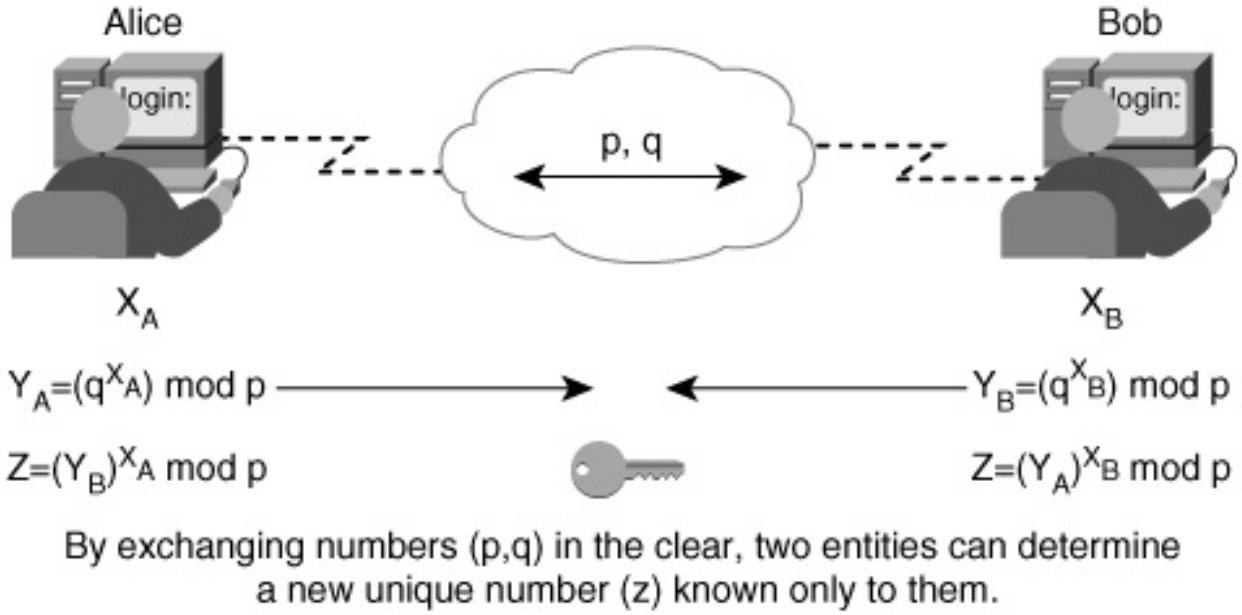

Figure 4.1: Diffie hellman protocol

4.1 Proposed Method

The IN_RAND is the vulnerable point of the whole algorithm. So instead of sending this unencrypted via air we can use the Diffie Hellman Protocol [14] to exchange this random number between the two devices. This protocol is basically a key exchange protocol but we have not applied this protocol directly on the key rather we are applying it on the random number and this random number will then be used in the generation of the key. So instead of applying the diffie hellman directly on the key we are applying it a step behind so as to make the system more secure.

4.2 Implementation

The project has been done in JSR-82 which is known as the java specification request.

The first screenshot shows the discovered bluetooth devices around.It starts a device enquiry and then discovers the address of all the added and the active

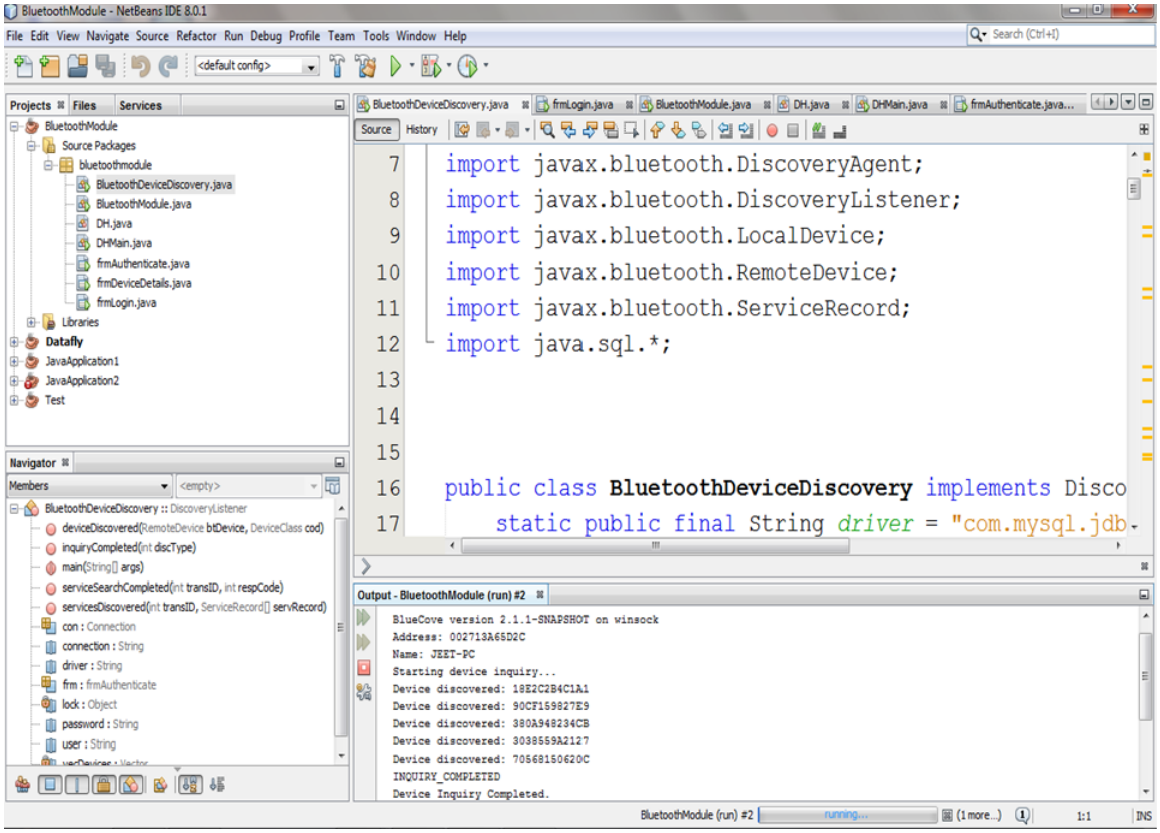

Figure 4.2: Device Enquiry(Screenshot-1)

bluetooth devices present around.After the enquiry is over it displays the bluetooth devices along with their names.

The second screenshot and the third screenshot show how the devices are added to the database of the bluetooth devices. A PIN is required for adding to the database.

The fourth screenshot shows the implementation of the diffie hellman protocol which is used on the IN_RAND(shown below).With this protocol finally the random number gets exchanged between the two devices.

The fifth,sixth and seventh screenshot show the final file transfer.

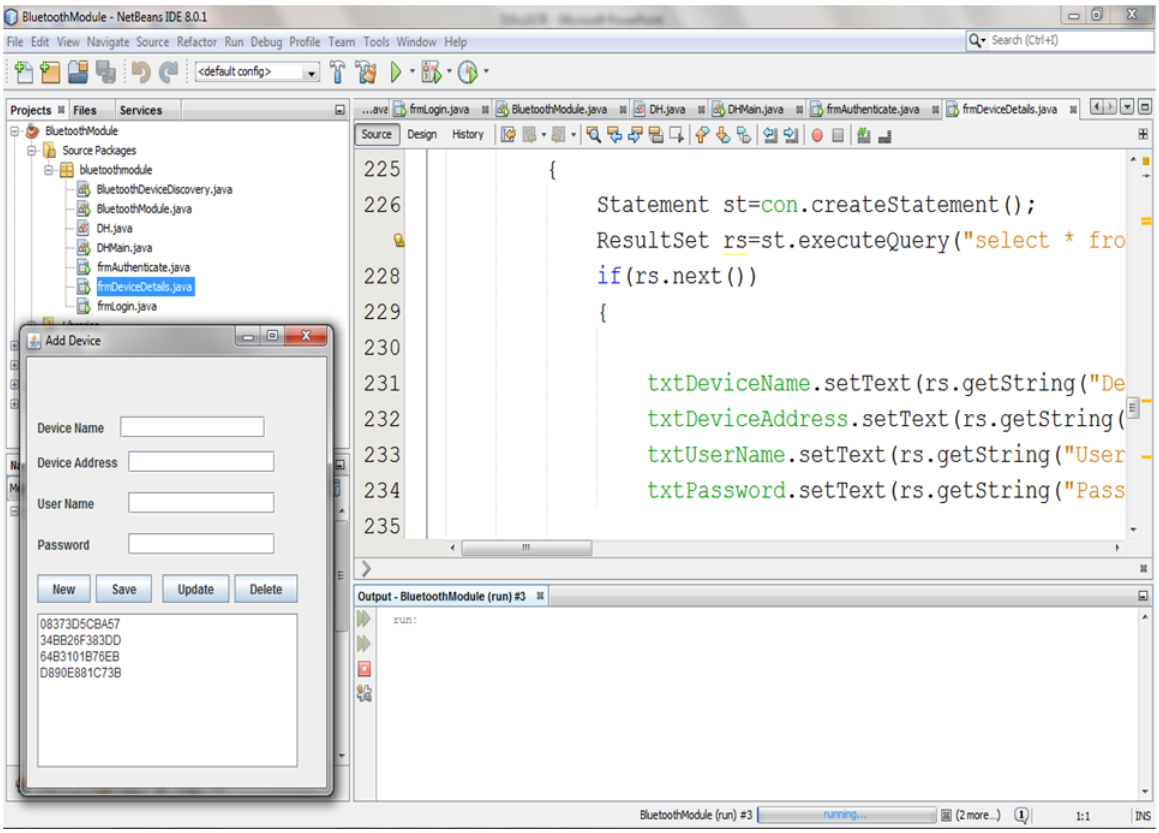

Figure 4.3: Add Device(Screenshot-2)

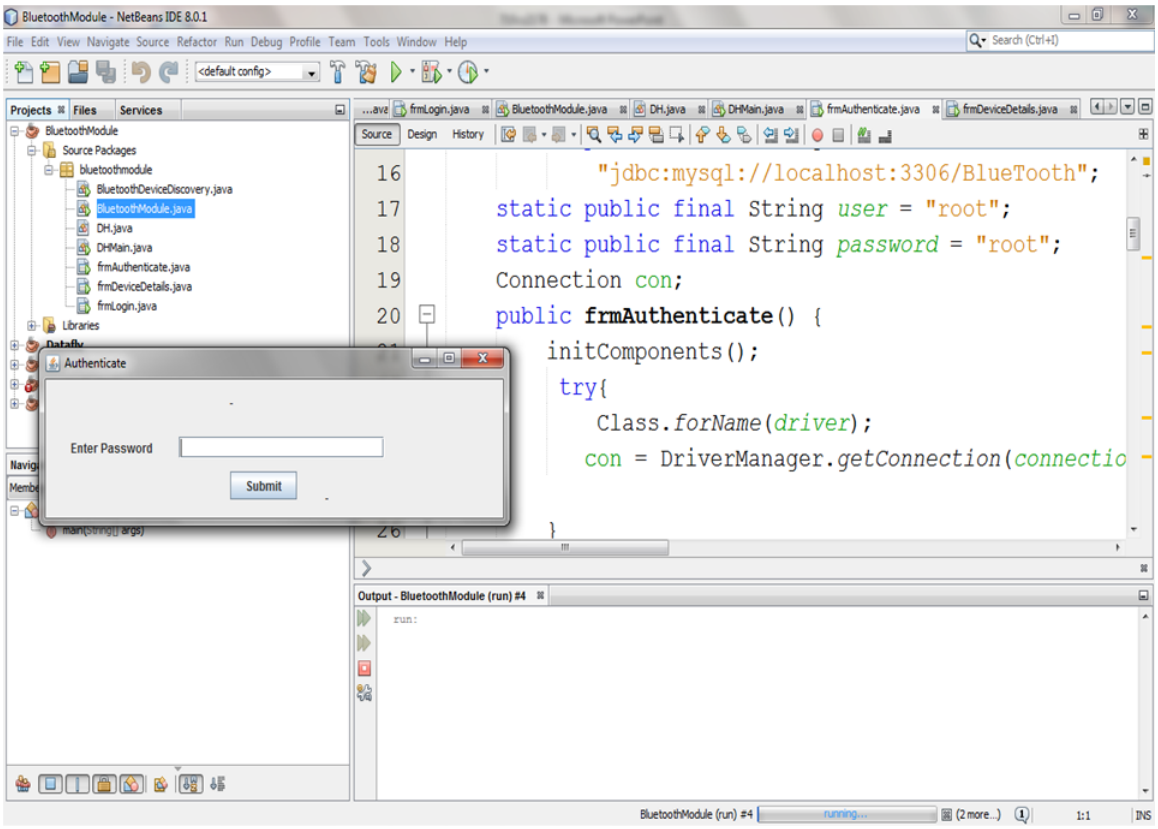

Figure 4.4: Enter Password(Screenshot-3)

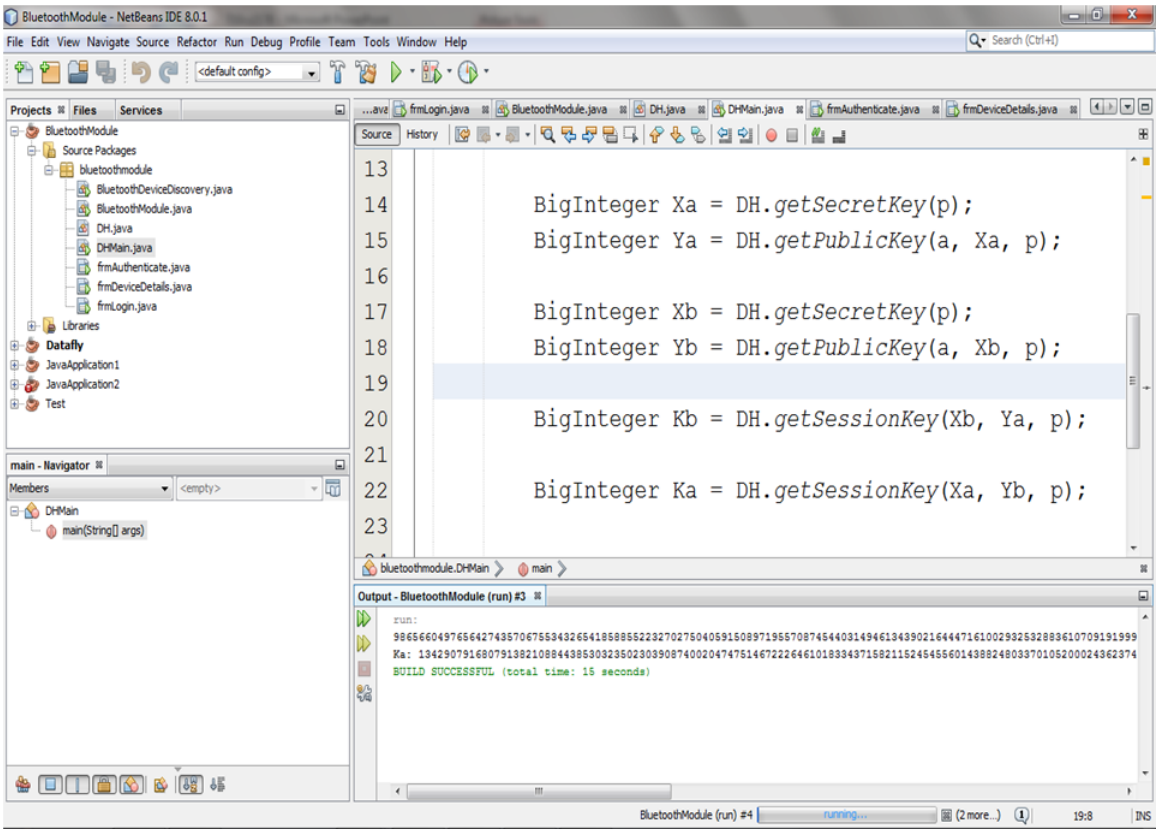

Figure 4.5: DH Protocol(Screenshot-4)

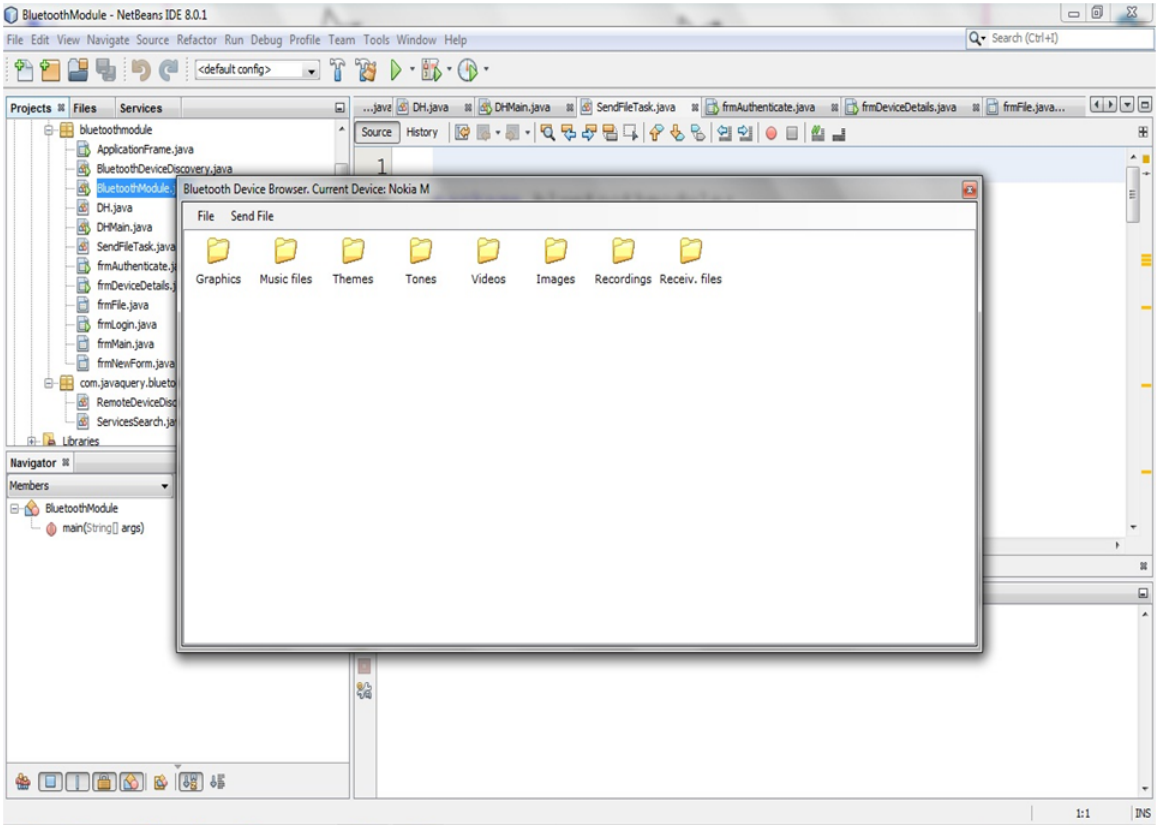

Figure 4.6: Contents of the other device(Screenshot-5)

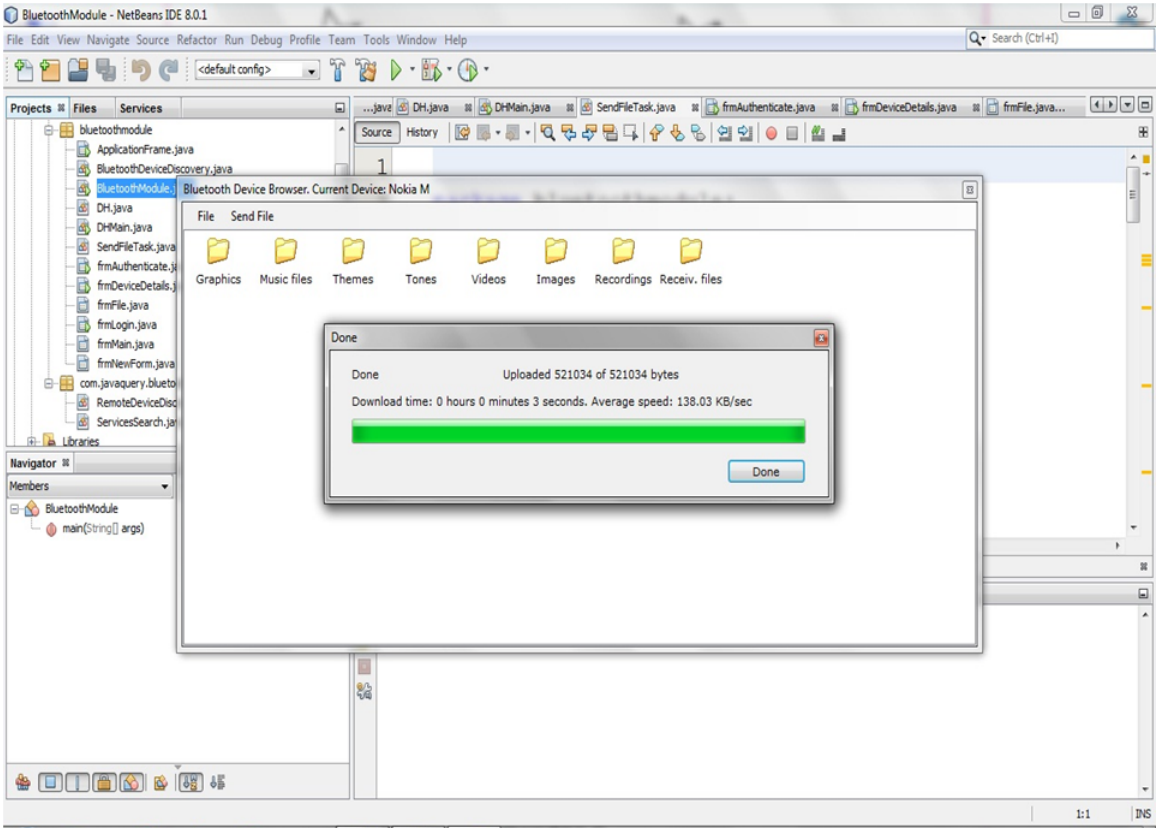

Figure 4.7: Uploading of the file(Screenshot-6)

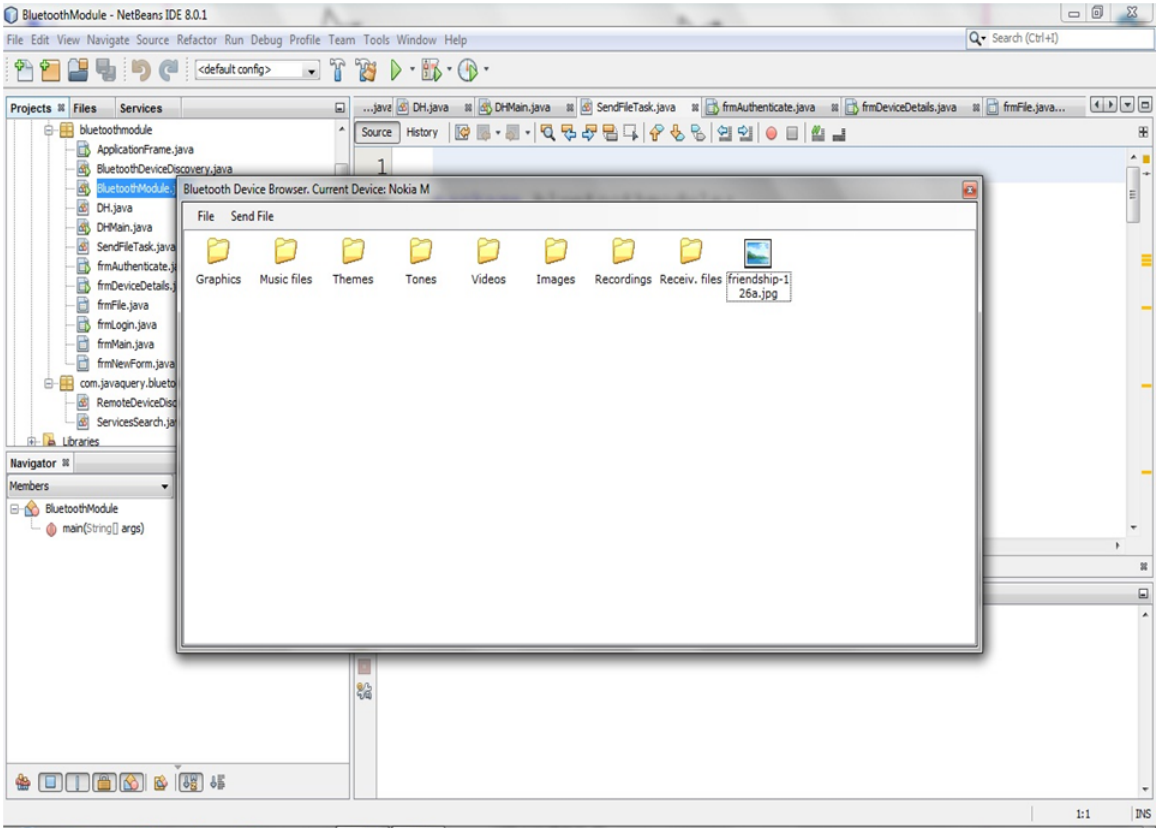

Figure 4.8: Image File Uploaded(Screenshot-7)

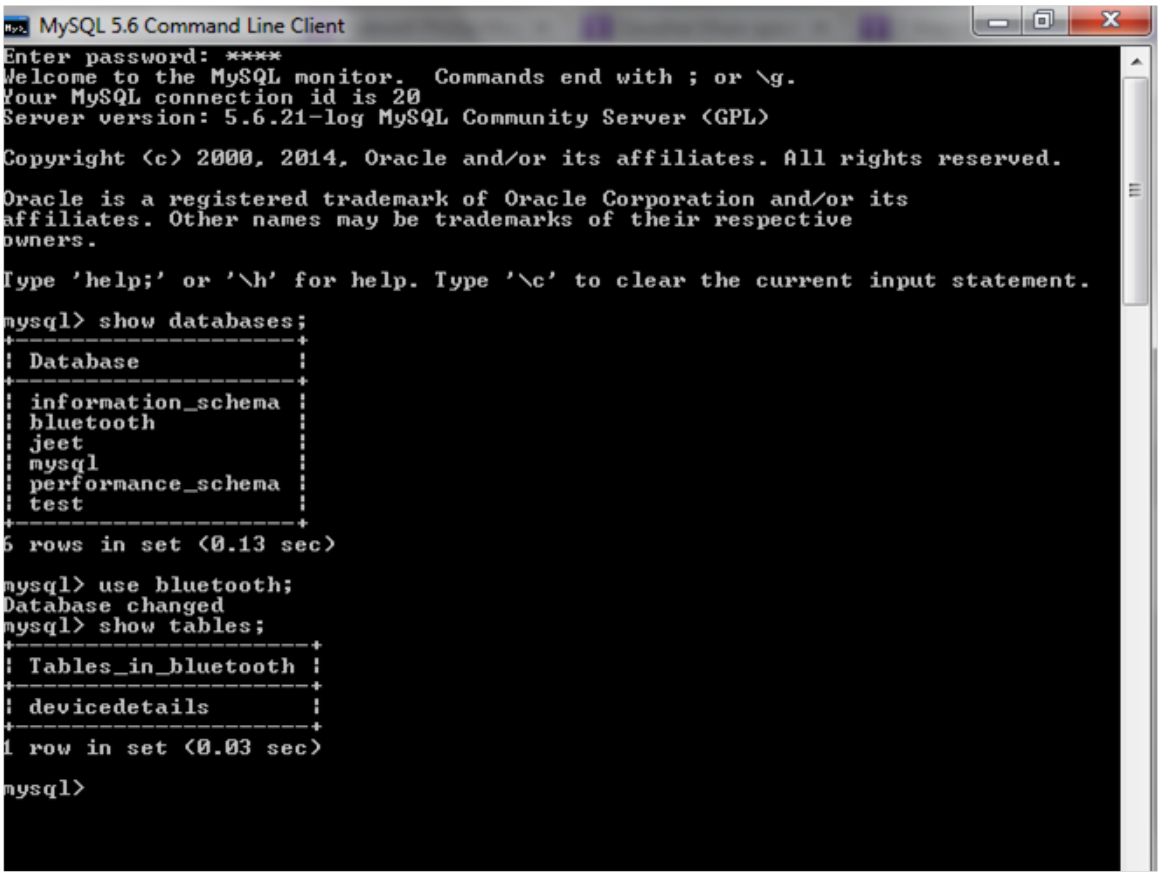

Figure 4.9: MySql(Screenshot-8)

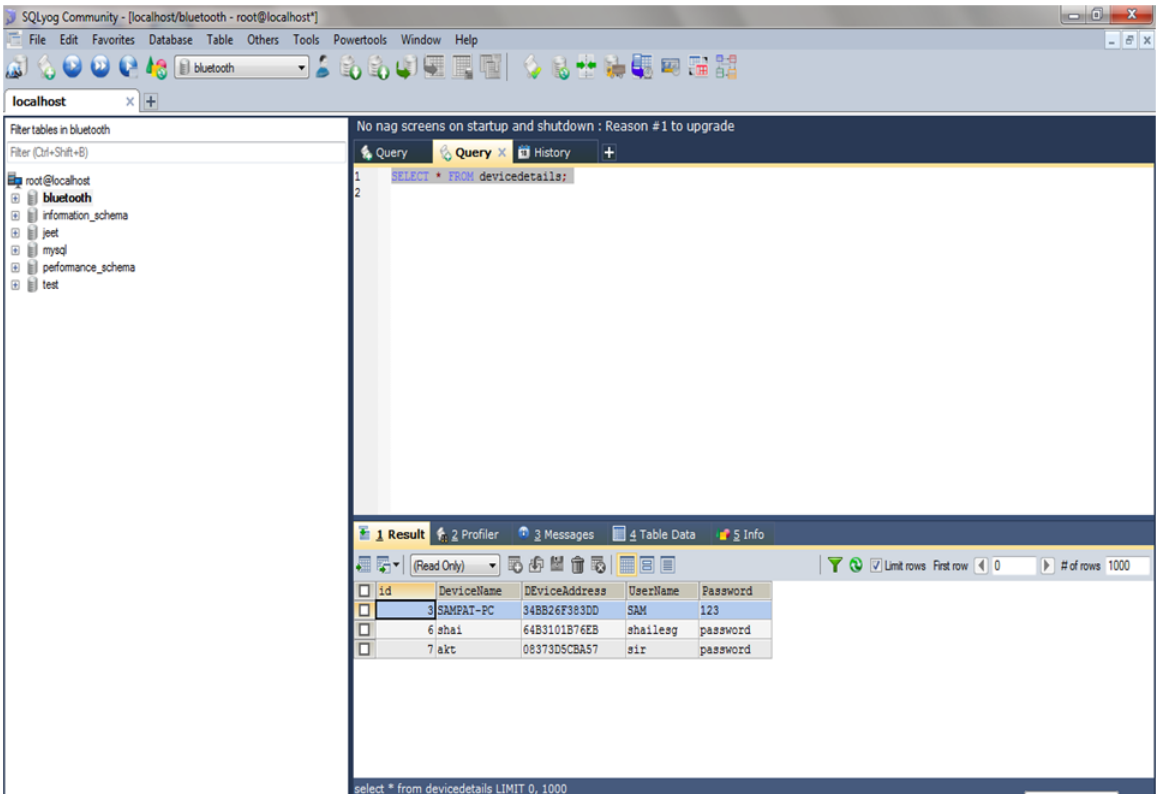

Figure 4.10: SQLYog(Screenshot-9)

The database used is MySql and SQLYog for grapical user interface.This is shown in the eighth and ninth screenshots.

Chapter 5

Conclusion

5.1 Achievements

So the file transfer was finally implemented using JSR-82. The proposed method is more secure than the one which is used in bluetooth in the present time. The randomness parameter of the VERDICT methodology is an important factor for determining the weakness of the bluetooth system. So our proposal is an improvement considering this parameter as it brings about more randomness in the generation of the random number.

5.2 Drawback and Future Scope

The random number IN_RAND was sent using the diffie hellman protocol. But Diffie Hellman protocol is also prone to the man in the middle attack so the algorithm can be further improved and it has scope of improvement.Bluetooth is relatively a new field and nowadays its used extensively so it needs to be fully explored.

Bibliography

[1] P.M. Barnaghi and S.S Liong. Bluetooth network security: A new approach to secure scatternet formation. *TENCON 2005 - 2005 IEEE Region 10 Conference*, pages 1–6, 2005.

[2] F. Ferro, E.and; Potorti. Bluetooth and wi-fi wireless protocols: A survey and a comparison. *Wireless Communications, IEEE*, 12(1):12–26, 2005.

[3] S. Sandhya and K.A.S. Devi. Analysis of bluetooth threats and v4.0 security features. *Network, IEEE*, 1:1–4, 2012.

[4] `http://www.jsr82.com`.

[5] Creighton T. Hager and Scott F. Midkiff. An analysis of bluetooth security vulnerabilities. *Wireless Communications and Networking, 2003. WCNC 2003, IEEE*, 3:1825–1831, 2003.

[6] Bruce Hopkins and Ranjith Antony. *Bluetooth for Java*. Apress, 1st edition.

[7] Creighton T. Hager and Scott F. Midkiff. Demonstrating vulnerabilities in bluetooth security. *Global Telecommunications Conference, 2003, IEEE*, 3:1420–1424, 2003.

[8] Yu Xin, Wang ZhaoShun, and Chu RongGong. Application of group key agreement based on authenticated diffie-hellman for bluetooth piconet. *Information Engineering, 2009. ICIE '09. WASE International Conference, IEEE*, 2:125–128, 2009.

[9] Anthony C Davies. An overview of bluetooth wireless technology and some competing lan standards. *Circuits and Systems for Communications, 2002. Proceedings. ICCSC '02.*, pages 206–211, 2002.

[10] Yu Xin and Yan Ting. A security architecture based on user authentication of bluetooth. *Information Technology and Applications, 2009. IFITA '09. , IEEE*, 3:627–629, 2009.

[11] K.Saravanan and D.Yuvaraj. An new secure mechanism for bluetooth network. *2nd International Conference on Computer and Automation Engineering (ICCAE), 2010*, 1:202–205, 2010.

[12] Minar, Nateq Be-Nazir Ibn, and Mohammed Tarique. Bluetooth security threats and solutions: A survey. *International Journal of Distributed and Parallel Systems*, 3:127–148, 2012.

[13] J.P. Dunning. Taming the blue beast a survey of bluetooth-based threats. *Security and privacy, IEEE*, 8(2):20–27, 2010.

[14] B. A. Forouzan and D. Mukhopadhyay. *Cryptography and Network Security.* Tata McGraw-Hill, 2nd edition.

[15] Christian Gehrmann, Joakim Persson, and Ben Smeets. *Bluetooth Security.* Artech House, 2nd edition.

[16] Trishna Panse and Prashant Panse. A survey on security threats and vulnerability attacks on bluetooth communication. *International Journal of Computer Science and Information Technologies*, 4(5).

[17] Rajveer Kaur and Rupinder Kaur Cheema. Enhancing bluetooth authentication using diffie hellman algorithm. *International Journal of Computer Applications*, 68(18).

[18] `http://en.wikipedia.org/`.

[19] `http://www.bluetooth.org/en-us/`.

[20] Vikas Gupta, Avinash Das, Deepesh Jain, and K.V.Prasad. *Cracking the Code:WAp,Bluetooth and 3G Programming.* Hungry Minds, 1st edition.

[21] Yan Zhang Ji Jun Daniel Kay Li, Tianji and Yang Xiao. Security issues in the ieee 802.15.1 bluetooth wireless personal area network. *Security in Distributed Grid Mobile and Pervasive Computing*, 2007.